Trustworthy Computing
Academic Advisory Board

July 30 – 31 2003

Agenda

- Introduction of Participants
- Administrative Details
  - Contacts – Dave Ladd x30404; Noelle Triou, x25575
  - Travel update
  - Videotaping
  - Confidentiality
- First Session - Status:
  - Progress on action items from last meeting
  - Introduction of Peter Cullen (New Privacy Officer)
  - Update on GeCAD acquisition
  - Update on Pelican acquisition
  - Update on Steve Lipner's changing role
  - Update on MSR management changes
  - Discussion of outstanding board slots
  - Discussion of latest critical bug fixes, processes, etc.
- Second Session – Threat Modeling 10:00am – 3:30pm
- Final Session – Windows Privacy Standard 4:00pm – 6:00pm
- Dinner – 7:00pm

Action Items

Procedural Commentary

- **Speaker Quality/Presentation Type**
  - Need to have senior leadership present for the entire meeting, so these people can get first-hand understanding of credibility of current technical staff and approach. (Senior people from presenting org need to be present in addition to Microsoft corporate management.) — **DONE - ONGOING**

- **Timing/length of discussion/format**
  - More and longer breaks — **DONE**
  - Two day meeting is okay; but fewer talks day two — **DONE**
  - First session should be for committee discussion — **DONE**
  - Have speakers be available at dinner reception — **DONE**
  - There was not enough time for informal discussions with speakers, following their talks — **DONE**
  - Longer board only session for summary needed — **DONE**

- **Other items**
  - Create an email alias for the board members — **DONE - Listserver**
  - We should get copies of slides after the meeting — **DONE - WEBSITE**
  - We should get copies of minutes after the meeting — **DONE - WEBSITE**
  - We should get copies of a to-do list based on topics raised in the meeting — **DONE - Action List**
  - Better read ahead package would be preferred — PARTIALLY DONE
  - Prefer to hear about things when we can still have impact — PARTIALLY DONE
  - Board should have the opportunity to have input on the agenda — **DONE - Action List**
  - We may want to change the composition of the board — OUTSTANDING

Action Items

Technical Commentary

- **STRIDE/Windows Security Push/Software Engineering Process**
  - Need to better understand the threat model, STRIDE, etc., and to understand the extent to which management and real programmers understand the virtues and limits of attack surfaces, etc. **DONE – THIS SESSION**
  - What is the whole software development process? In particular, design and architecture is part of the process and we need to see how security and privacy concerns come into play here. FUTURE SESSION
  - Revisit the security push process vis a vis long term culture change. OPEN QUESTION
  - Bring in MS technical education to hear their views on how teachable this stuff is FUTURE SESSION
    - Revisit the extent to which training and security push is becoming pervasive in the corp.
  - Assurance: How does Microsoft measure whether security is increasing/improving? OPEN QUESTION
- **Longhorn**
  - There are lots of parts of Longhorn to discuss. Two obvious ones: FUTURE SESSION
    - New authorization architecture
    - Reboot discussion
- **Privacy**
  - How to "operationalize" the privacy policy; Can it be handled like a threat analysis? **THIS SESSION**
  - How do technical and legal policies and cultures interact? FUTURE SESSION
    - Test case: privacy in Palladium?

SD³ At Work – MS03-007

Windows Server 2003 Unaffected

The underlying DLL (NTDLL.DLL) not vulnerable	Code made more conservative during Security Push
Even if it was vulnerable	IIS 6.0 not running by default on Windows Server 2003
Even if it was running	IIS 6.0 doesn't have WebDAV enabled by default
Even if it did have WebDAV enabled	Maximum URL length in IIS 6.0 is 16kb by default (>64kb needed)
Even if the buffer was large enough	Process halts rather than executes malicious code, due to buffer overrun detection code (/GS)
Even if it there was an exploitable buffer overrun	Would have occurred in *w3wp.exe* which is now running as 'network service'

SD³ At Work – MS03-007

Windows Server 2003 Unaffected

The underlying DLL (NTDLL.DLL) not vulnerable	Code made more conservative during Security Push
Even if it was vulnerable	IIS 6.0 not running by default on Windows Server 2003
Even if it was running	IIS 6.0 doesn't have WebDAV enabled by default
Even if it did have WebDAV enabled	Maximum URL length in IIS 6.0 is 16kb by default (>64kb needed)
Even if the buffer was large enough	Process halts rather than executes malicious code, due to buffer overrun detection code (GS)
Even if it there was an exploitable buffer overrun	Would have occurred in *w3wp.exe* which is now running as 'network service'

Action Items

Technical Commentary

- **STRIDE/Windows Security Push/Software Engineering Process**
  - Need to better understand the threat model, STRIDE, etc., and to understand the extent to which management and real programmers understand the virtues and limits of attack surfaces, etc. **DONE – THIS SESSION**
  - What is the whole software development process? In particular, design and architecture is part of the process and we need to see how security and privacy concerns come into play here. FUTURE SESSION
  - Revisit the security push process vis a vis long term culture change. OPEN QUESTION
  - Bring in MS technical education to hear their views on how teachable this stuff is FUTURE SESSION
    - Revisit the extent to which training and security push is becoming pervasive in the corp.
  - Assurance: How does Microsoft measure whether security is increasing/improving? OPEN QUESTION
- **Longhorn**
  - There are lots of parts of Longhorn to discuss. Two obvious ones: FUTURE SESSION
    - New authorization architecture
    - Reboot discussion
- **Privacy**
  - How to "operationalize" the privacy policy: Can it be handled like a threat analysis? **THIS SESSION**
  - How do technical and legal policies and cultures interact? FUTURE SESSION
    - Test case: privacy in Palladium?